IN THE CLAIMS:

Amended claims follow:



1. (Currently Amended) A method for detecting potentially harmful actions on a handheld computer, the method comprising:

monitoring calls to applications resident on the handheld computer; identifying a code associated with a program initiating said call; and at least temporarily preventing an action requested by said call from being executed if the identified code does not correspond to a code associated with data said action is to be performed upon; wherein identifying a code comprises identifying a creator code on a handheld computer operating system;

wherein the creator code is used to prevent malicious behavior.

- 2. (Original) The method of claim 1 wherein monitoring calls to applications comprises installing a patch on the handheld computer, the patch being operable to intercept calls.
- 3. (Original) The method of claim 2 wherein installing a patch comprises replacing an API address with a patch address.
- 4. (Original) The method of claim 2 wherein installing a patch comprises utilizing get trap and set trap commands.
- 5. (Cancelled)
- 6. (Original) The method of claim 1 further comprising identifying at least one of the applications as a trusted application, wherein trusted applications are not prevented from performing actions.
- 7. (Original) The method of claim 1 further comprising receiving data on an infrared port of the handheld computer and installing said data in a temporary database.

Docket NAI1P137/00.123.01



- 8. (Original) The method of claim 7 further comprising asking a user whether to accept said data before loading said data onto the handheld computer.
- 9. (Original) The method of claim 1 wherein the action requested is a password manipulation.
- 10. (Original) The method of claim 1 wherein the action requested is deletion of data.
- 11. (Original) The method of claim 1 wherein the action requested is modification of data.
- 12. (Original) The method of claim 1 wherein the action requested is manipulation of an operating system.
- 13. (Currently Amended) A method for detecting potentially harmful actions on a handheld computer, the method comprising: monitoring requests for action by applications on the handheld computer; evaluating said requests to determine if said requests may result in potentially harmful behavior to data stored on the handheld computer;

preventing said action from being performed if said request is identified as potentially harmful behavior; and

notifying a user of the handheld computer of said potentially harmful behavior;

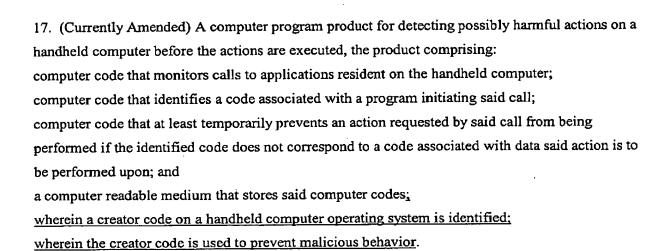
wherein evaluating said requests comprises comparing a creator code associated with the application requesting said action with a creator code associated with data the action is to be performed upon; wherein the creator code is used to prevent malicious behavior.

- 14. (Original) The method of claim 13 wherein monitoring requests for action comprises monitoring API calls.
- 15. (Cancelled)
- 16. (Original) The method of claim 13 further comprising identifying at least one application as a trusted application and allowing said action to be performed even if said request is identified as potentially harmful if requested by the trusted application.

Docket NAI1P137/00.123.01

3







18. (Original) The computer product of claim 17 further comprising code that identifies at least one of the applications as a trusted application and wherein trusted applications are not prevented from performing actions.

19. (Cancelled)

20. (Currently Amended) A computer program product for detecting possibly harmful actions on a handheld computer before the actions are executed, the product comprising: computer code that monitors requests for action by applications on the handheld computer; computer code that evaluates said requests to determine if said requests may result in potentially harmful behavior to data stored on the handheld computer; computer code that prevents said action from being performed if said request is identified as potentially harmful behavior; computer code that notifies a user of the handheld computer of said potentially harmful behavior; and a computer readable medium that stores said computer codes; wherein evaluating said requests comprises comparing a creator code associated with the application requesting said action with a creator code associated with data the action is to be performed upon;

Docket NAI1P137/00.123.01

wherein the creator code is used to prevent malicious behavior.